The Other Side of Privacy: Surveillance in Data Control

Rula Sayaf
Department of Computer Sciences, DistriNet–iMinds
KULeuven, Belgium
rula.sayaf@cs.kuleuven.be

Dave Clarke
Department of Information Technology
Uppsala University, Sweden
dave.clarke@it.uu.se

James B. Rule
The Center for the Study of Law & Society, Berkeley Law
University of California, USA
jbrule@berkeley.edu

ABSTRACT

Privacy and surveillance take on new forms through social software technologies. Privacy may not be achieved by being let alone, rather, by choosing a group of people whom are trusted with one's data. Similarly, surveillance takes the form of monitoring users' data rather than monitoring users themselves. To offer privacy and counter surveillance, the "privacy as control" paradigm focuses on approaches that offer as much data control as possible. In practice, offering control to users depends on assigning control to non-user entities, who may have surveillance capabilities, which results in an interdependency of privacy and surveillance. This interdependency is problematic and contradicts what data control approaches should offer. In this paper, we examine this interdependency in data control within social software. We put forward criteria to evaluate the degree of control and privacy and the degree of surveillance entailed by a data control approach. We perform a comparative analysis of data control approaches in the technical and the legal context. The analysis shows how certain aspects of surveillance are deeply rooted in the realisations of "privacy as control". We argue that data control approaches should offer transparency, reciprocity and a balanced degree of control as a first step towards addressing the interdependency of privacy and surveillance.

CCS Concepts

•Security and privacy → Human and societal aspects of security and privacy; • Social and professional topics → Privacy policies; Surveillance; •Networks → *Online social networks;* **•Information systems** → *Data access methods;* Database administration; **•Social and professional topics** → Government technology policy; Internet governance;

British HCI 2015, July 13 - 17, 2015, Lincoln, United Kingdom

DOI: http://dx.doi.org/10.1145/2783446.2783584

Keywords

Privacy, surveillance, data control, social software, privacy as control, the EU Data Protection Directive

1. INTRODUCTION

The concepts of privacy and surveillance take new forms in social software technologies. Privacy and surveillance are two important concepts in relation to data disclosure and communication. Traditionally, privacy refers to the right of an individual to be isolated or anonymous [32, 20]. Through privacy, it is possible to avoid surveillance. However, the nature of social software communication affects how these two concepts are viewed and practiced. In social software, privacy may not be achieved through being alone if one is to use the software. Rather, it is a compromise between disclosing data to a set of trustees and hiding it from others. Surveillance takes a new form of monitoring users through their data disclosure. Surveillance is achievable through the utilisation of social software to monitor users. In such cases, privacy may not necessarily counter such surveillance [7].

"Privacy as control" (PaC) is one of the most fundamental aspects of daily use of social software. PaC is a research paradigm of privacy management approaches through data control [10]. Social software users can disclose their personal data to various types of audiences. To manage their privacy, users can employ data control approaches. Data control approaches offer users control on where and to whom their data is disclosed to avoid inappropriate access, tracking, and surveillance. Data control approaches include two classes, namely, access control and accountability. Access control offers means to control who can access data, how, and for what purpose. Accountability offers the verification of the correct enforcement of data control users have. Data control approaches are realised in different ways in technical and legal frameworks.

Although PaC aims at facilitating privacy, in practice, it involves a certain degree of surveillance. PaC approaches are realised differently in technical and legal frameworks. In the two frameworks, giving total control to users is challenging and may not be feasible [26]. In the technical framework, the complexity of data control approaches requires involving *functional entities*—other than users—to deploy these approaches. Such entities control users' data and monitor their actions. With such control, functional entities have surveillance powers. In the legal framework, similar entities are required to monitor users to enforce the laws and detect violations. We refer to the surveillance that is required for the functioning of data control approaches as *functional*

surveillance. Functional surveillance is essential to ensure privacy management. At the same time, there is no guarantee that functional surveillance may not be used for surveillance of users. In such a case, functional surveillance can turn the social software into a panopticon [14].

The interdependency of privacy and surveillance hinders the assessment of the degree of control and privacy users can have. Functional surveillance in PaC demonstrates an interdependency of privacy and surveillance. While privacy aims at countering surveillance, it may utilise functional surveillance. Functional surveillance can facilitate and hinder privacy. As a result, the control required by functional entities may limit users' control. Functional surveillance affects the offerings of data control approaches and their effectiveness. The main challenge to assessing the offerings of data control approaches is that control is an abstract concept. Control cannot be quantified; however, it can be assessed by the aspects it affects. In this article, we investigate the degree of control, privacy and the related surveillance issues. Our contribution can be summarised as follows:

- Presenting PaC in theory and in practice, and discussing the limitations of PaC core principle (Section 2);
- Presenting the main characteristics of data control approaches and proposing criteria to assess the possible degree of control (Section 3);
- Evaluating the criteria by applying them in the technical and legal frameworks (Section 4);
- Demonstrating that transparency and reciprocity are the most essential requirements towards addressing the interdependency of privacy and surveillance (Section 5).

2. PRIVACY AS CONTROL

"Privacy as control" (*PaC*) is one of three research paradigms of privacy management approaches in the technical and legal frameworks [10]. "Privacy as confidentiality" and "privacy as practice" are the other two. Privacy management approaches vary across paradigms in their approach, assumptions and objectives. In this article, we only focus on the PaC paradigm and data control approaches—as opposed to anonymity, feedback, and awareness approaches that belong to the other two paradigms [10]. Our focus aims to investigate the interdependency of privacy and surveillance rooted in data control approaches in social software.

2.1 PaC in Theory

Theoretically, PaC concerns offering users as much control as possible to control their data and disclosure contexts in social software. Users can disclose their data in communication contexts within the software. These data can be accessed and may be used inappropriately. To manage their privacy in social software, users should be able to control their data, in terms of how it is accessed and handled in contexts [25].

Controlling context means that a user should be able to control the various ingredients in a context [25]. In social software, a *context* is the information that identifies a situation within which a user can disclose a data item. For example, in Facebook, a context is the information in a page within which a user posts her graduation photo. The context is defined by the data, the poster and the audience. The *poster* discloses a data item and selects the audience. The *audience* is the set of users who can view an item of a specific poster. A *data subject* is a user that the item relates to, referred to as a subject in this article. Generally, the poster discloses data for which she is the subject. However, it is possible to post items about others; we refer to those subjects as *participants*. Participants can also be members of the audience who contribute to the context with their data, e.g., post comments. Controlling context, a user should be able to control the context ingredients in the *original context*, wherein the data is first disclosed and any dissemination context [25].

2.2 PaC in Practice

In practice, PaC is realised by data control approaches to offer control to users over their data. Data control approaches aim at facilitating the expression, the enforcement, and the verification of users' control over their data. Expressing control over data requires verifying the correct observance of this control. Access control and accountability approaches offer users various aspects of control. Access control approaches enable users to control access to their data. Accountability approaches verify the enforcement of users' control and identify misconduct.

Data control approaches offer a varying degree of data control. Based on the assumptions and objectives of an approach, the degree of control varies [26]. In many cases, these approaches involve functional entities that perform particular functionalities, e.g., an access control enforcement entity or an accountability and audit entity. Functional entities are necessary in certain approaches to perform tasks that users are unable to perform. Functional entities are required to have a certain degree of data control to perform their tasks. With such control, functional entities have access to users' data and actions. This control, in turn, limits the degree of control users can have, e.g., by not allowing users to hide their data from functional entities. Moreover, the realisations of these approaches and their offerings vary based on the underlying framework. Such variance means that a consistently high degree of control is not possible in PaC in practice, as we discuss next.

2.3 Limitations of PaC and Surveillance

The main issue of PaC is that it may not be practically possible to offer a high degree of control to social software users [10]. In practice, users may be faced with various limitations. Such limitations can be technical, legal, and ethical. From a technical point of view, the degree of control depends on the capabilities of the social software system, the design of the data control approach, and the data it protects. Additionally, the degree of control depends on the usability of the approach. In general, users face difficulties in using PaC approaches [24]. However, in the context of this article, we do not focus on the usability issues of PaC. From a legal point of view, the degree of control varies depending on international boundaries, e.g., there is a significant difference between the control offered by the EU Directive and the US privacy legislations [23].

From an ethical point of view, assigning a high degree of control to users may have counter-privacy consequences [26]. Users with a high degree of control can conceal their malicious acts of violating others' privacy, e.g., leaking data. In such a case, assigning a high degree of control to users can

run counter to what is dictated by law. According to the law, when data may affect other users or concerns criminal or illegal acts, a certain degree of supervision and the limitation of users' control are needed. Supervision of users' actions can be achieved by accountability approaches, for instance. Such approaches entail a certain degree of surveillance.

Social software may be utilised for different forms of surveillance. Social software are seen as a realisation of surveillance in the modern society [11]. Many parties can apply surveillance such as parents, marketing, recruiting companies or governments [3]. This form of surveillance is achievable through monitoring the data users disclose. Another form of surveillance is functional surveillance achievable through PaC. Functional surveillance is a fundamental part of many data control approaches (Section 3). Functional surveillance facilitate monitoring users disclosures, actions, trust and privacy management patterns.

The main challenge is that it is not possible to assess the degree of control the users and other parties could have, and the involved degree of functional surveillance. Both users and researchers need to understand the offering of data control approaches. The inability to assess the degree of control users can have affects assessing the degree of privacy management that can be achieved. To address this problem, an understanding of data control approaches is needed. Based on such understanding, it is possible to assess—at a high level—the control users can have and functional entities can have. In the following, we provide an understanding of data control approaches and propose criteria for evaluating the control offered to users and the entailed functional surveillance. We apply the criteria on the general aspects of data control approaches at a high level. Such an application demonstrates how the criteria can be used to asses any data control approach.

3. DATA CONTROL APPROACHES

Data control approaches are means that allow users to control how their data is handled. These approaches include access control and accountability approaches. In the following, we discuss the realisations in the technical and legal frameworks.

3.1 The Technical Framework

The technical framework realises data control approaches via technical mechanisms to express, enforce and verify data control, as described in the following.

3.1.1 Access Control

An access control mechanism enables users to control their data. The control is achieved by composing policies based on a specific set of features in the system to regulate and authorise access to data [24]. For instance, a policy can state that only users who are of a certain age can access a specific data item. Most of the mechanisms assign control to the poster assuming that the poster is the subject. Fewer mechanisms may assign control to posters and participants, i.e., the mechanism of Squicciarini et al. [29]. For each access request of a data item, the relevant policy of the controller is enforced. When the constraints of the policy are satisfied, access is authorised. The enforcement of policies is executed by an enforcement mechanism. The enforcement mechanism or entity is a functional entity that controls users' data and policies.

An access control mechanism may involve one or more functional entities depending on the social software architecture. In *centralised architectures*, a central authority is responsible for providing the social software services. The central authority can be the enforcement functional entity. In *decentralised architectures*, the data is distributed on multiple servers. These entities are the functional entities. Another option is deploying the services on users' own machines, i.e., the work of Cutillo et al. [6]. In this case, the user machine acts as a functional entity.

3.1.2 Accountability

Accountability mechanisms are based on auditing the system to identify misconduct and anomalous actions [28]. These mechanisms perform auditing of system logs, policy enforcement transactions and users' actions. By such auditing, they reason about compliance with privacy rules [27]. When no violations are detected, it is an indication of observance of the control users have expressed.

The functioning of accountability mechanisms requires the involvement of functional entities. The number of functional entities depends on the social software architecture. In *centralised architectures*, the central authority is the functional entity that deploys the mechanism. This entity tracks users' actions. In *decentralised architectures*, the entities hosting the social software are required to cooperate and exchange data. These entities have to record all the information exchanged between users and then link them to data of other entities [13].

3.2 The Legal Framework

The legal framework adopts PaC through data protection legislation to protect individuals [1]. We focus on the legislation of the European Directive 95/46/EC (EU Directive 1995), referred to as "the directive" in this article. The directive is (in comparison to other data protection legislation) one of the most privacy-friendly legal regulations [23].

3.3 Access control and Accountability

The directive offers data protection via adopting accountability [2]—and implicitly access control. The directive states the rights and liabilities of entities that can access and process data. By specifying who can access and process data, the directive also formulates access control regulations.

The directive differs from the technical framework by the set of entities that can have control over data. Instead of assigning control to users, the directive distinguishes two main entities: the data subject and the data controller. The controller "determines the purposes and means" of the processing (Article 2(d)), and is responsible for ensuring compliance with the directive. In contrast to the technical framework, the directive considers the social software provider or a third party to be the controller. Subjects are not considered the data controllers of their own data. According to the personal use exemption (Article 3(2))—when data is accessed for "purely personal or household activities"—subjects are not the data controller of their own data. Subjects may not solely determine the purposes and means of the processing of their data. However, subjects can be considered as controllers of other subjects' data, not their own [5].

The directive distinguishes between controlling and processing data. The directive defines a data processor role as the entity that can process and perform specific operations

on data on behalf of the controller. The processor is usually not a subject. Although the data controller can solely determine how subjects' data is processed, subjects have the right to be informed and give consent to the control of the data controller (Article 7). The data controller is obliged to inform subjects about its identity and purpose of processing in order to obtain their consent (Articles 10–11). The data controller should maintain the accuracy of data or else delete or rectify them. However, the data controller is not subject to those constraints in specific exceptional cases (Articles 13, 7(b–f)). The first exception (Article 13) applies when the processing of data is necessary for the completion of tasks of legal authorities, such as the protection of the security or economic interests of the state, criminal investigations, or the protection of subjects, their rights and freedoms. The second exceptional case (Article 7(b–f)) applies when the processing is required to comply with a contract the subject is part of, fulfil a legal obligation, or protect the interest of the subject or the controller.

The legal framework varies from the technical framework in terms of the control they offer. The legal framework assigns the highest degree of control to the service provider, who is also a functional entity. In a distributed architecture, the number of service providers increases, and thus the number of functional entities.

4. EVALUATION CRITERIA FOR COMPLIANCE WITH PAC

Measuring the degree of fulfilment of PaC is not possible in general [10]. However, it is possible to assess the degree of control offered by a data control approach by investigating the aspects that can be controlled and the degree of functional surveillance entailed. According to the identified context ingredients (Section 2) and a previously proposed set of requirements for offering a high degree of control and privacy [24], we propose the following criteria. Each of the following criteria concerns a particular set of data control aspects.

Control over Data Which types of data items can a subject control? What subjects have control over their data, posters or participants? And what is the degree of control the subject has? Data items can be posted items, actions produced while using the social software, or other inferable data.

Identifiability of the Data Subject Is the subject identifiable in the original context? Is the subject identifiable in any dissemination context where her data is put?

Audience Control What is the degree of control a subject has over her audience? And what is the degree of control the audience have over the subject they are the audience of? Such control means that an audience member can select the subject to view data from.

Control over Context What is the degree of control a subject has over the original context within which her data is first disclosed? And what is the degree of control over any dissemination context? The degree of satisfaction of this criteria is dependent on the satisfaction of the above criteria. As an example, when participants cannot control their data, this criterion is not satisfied in relation to participants.

Degree of Functional Surveillance What is the degree of functional surveillance applicable by a functional entity?

In the following we evaluate the proposed criteria. For each criterion, we discuss the related aspects and state the approximate degree of satisfaction. The degree of control can be either, high, moderate or low. If the evaluation results in a high degree of control and a low degree of functional surveillance, we conclude that users can have a high degree of control, and in principle a high degree of privacy. The evaluation does not focus on a particular realisation, rather, it is performed at a high level on the general aspects shared amongst realisations. By this evaluation, we demonstrate how to perform the evaluation at a fine-grained level on a particular realisation.

4.1 Evaluating the Technical Framework

The criteria are applied on the main characteristics of technical data control mechanisms.

4.1.1 Evaluating Access Control

In the following, the satisfaction of the criteria is assessed on the main characteristics shared amongst various access control mechanisms, surveyed in [24].

Control over Data Access: Most mechanisms offer posters control over their posted data items. In relation to offering control to participants, only very few mechanisms offer such control [24], e.g., voting-based access control [31]. This criterion is satisfied to a high degree in terms of controlling the data users disclose, and to a low degree in terms of controlling actions or inferable data. It is satisfied to a high degree in terms of giving control to posters, and to a low degree in terms of giving control to participants.

Identifiability of the Data Subject: Most mechanisms maintain posters' identifiability in the original context, unless anonymous mechanisms or sticky policies are used [15]. Identifiability is maintained through the policies of the poster. The identifiability is not always possible in dissemination contexts. The lack of participants' control over their data makes them not identifiable. This criterion is satisfied to a high degree in the original context, and to a low degree in any dissemination context in relation to posters.

Audience Control: Access control mechanisms offer subjects control over their audience. This control is mainly offered to posters. The control is applicable within the social software boundaries. Posters' control does not apply to functional entities and what they may access [12]. It is not alway possible for the audience to have control over subjects. An example is Facebook-like access control, once a poster specifies the audience, the audience will have the poster's item in their newsfeed. The audience cannot specify the poster and what of her data they would like to view. This criterion is satisfied to a moderate degree in terms of giving control to posters over the audience to a low degree in terms of giving control to participants, but is not satisfied in terms of giving control to the audience.

Control over Context: Most mechanisms offer a high degree of control over the original context to posters, and a limited control over dissemination contexts [25]. Offering control over dissemination contexts to users requires assigning

a higher degree of control to functional entities over users' data and the contexts [30]. This criterion is satisfied to a high degree in terms of controlling the original context, and often a low degree in terms of controlling dissemination contexts.

Degree of Functional Surveillance: the degree of functional surveillance depends on the underlying architecture. In a centralised architecture, the enforcing entity must have access to users' posted data — unless the approach incorporates encryption to hide the content of the posted data. Upon enforcing a policy, the entity gains knowledge about who is denied or allowed to access a particular data item. The enforcement entity could infer information about users' trust patterns, amongst other information. In this architecture, the degree of functional surveillance is high due to possible accessibility of users' disclosed, actions or inferable data.

In decentralised architectures, users' data and actions are accessible by more than one functional entity. Even when these entities have access to a subset of the information, they can still aggregate the information. The challenge in this architecture is defining "trust" and "trusted entities". With the assumption that the trusted entities act as trusted and do not aggregate users' data, the functional surveillance is lower than that encountered in the central architecture. If the trusted entities aggregate users' data, the degree of functional surveillance is higher. In the case of deploying the enforcement mechanism on the user's own machine, no external functional entities are required and the degree of functional surveillance is low.

Access control mechanisms involve a relatively high degree of functional surveillance. This degree adds up to the degree of the control resulting in a moderate degree of control offered to users. The limited control offered to users is dependent on the control offered to functional entities. The more control functional entities have, e.g., over contexts inside and outside the social software, the more control users can have.

4.1.2 Evaluating Accountability

In the following, the satisfaction of the criteria is assessed on the main characteristics shared amongst various accountability mechanisms, surveyed in [1].

Control over Data: Accountability mechanisms facilitate indirect verification of subjects' control over only their posted data. Since subjects cannot define policies over actions, or inferable data (Section 4.1.1), accountability mechanisms cannot verify control over such data. Since participants cannot specify policies over their data, most accountability mechanisms can only verify the observance of posters' control. This criterion is satisfied to a high degree in relation to posted data to posters, and is not satisfied in relation to actions or inferable data.

Identifiability of the Data Subject: Accountability mechanisms are based on the identifiability of subjects. To identify accountable entities and the affected entities, every action and data is linked to its subject. However, the identifiability is mainly possible to the poster. This criterion is satisfied to a high degree in relation to posters, and to a lower degree in relation to participants.

Audience Control: Generally, these approaches check the handling of data by other users but not the functional entities [12]. Thus, these mechanisms verify the subject's control over the audience within the software. Accountability mechanisms do not check the audience control over their subjects when such control is missing in the access control mechanism. This criterion is satisfied to a high degree in terms of subjects controlling the audience, and is not satisfied in terms of the audience controlling subjects.

Control over Context: Accountability mechanisms can facilitate indirect control over data even in contexts that subjects do not have control over via access control mechanisms. When a data item is leaked into a new context, accountability mechanisms can detect the leakage in this context and report it to the subject concerned. The subject can take the appropriate action and thus have a certain degree of control. This criterion is satisfied to a higher degree by accountability mechanisms than by access control mechanisms.

Degree of Functional Surveillance: accountability mechanisms are strongly coupled with surveillance. The surveillance in these approaches takes the form of monitoring users' data and actions in order to identify misconduct. The degree of functional surveillance is dependent on the architecture. In a centralised architecture, the auditing entity has access to all users' data. In decentralised architectures, the functional entities have access to a subset of the data. Also, functional entities might need to aggregate data to identify misconduct, e.g., when a data item is leaked from one user to others, the auditing entities should aggregate their data to trace how the data item has moved from one user to another. This architecture entails a higher degree of functional surveillance than that of the centralised architecture.

Accountability mechanisms offer a moderate degree of control. At the same time, they comprise a higher degree of functional surveillance. In access control, users do not have control over who can access their actions and relational data. Yet, such data is utilised by accountability mechanisms to verify the observance of users' control over their posted data. Accountability mechanisms involve a high degree of functional surveillance by utilising the uncontrollable data to verify the control over controllable data.

In summary the technical framework offers a high degree of control on internal audiences and original contexts. At the same time, the framework involves a high degree of functional surveillance. Thus, the degree of total privacy achieved in this framework is moderate.

4.2 Evaluating the Legal Framework

In the following, the criteria are applied on aspects of access control and accountability regulations in the directive.

4.2.1 Evaluating Access Control

The criteria are satisfied to variant degrees as discussed in the following.

Control over Data: Subjects have control over any identifying data whether posted or processed by automatic means (Article 3(1)). The control is possible for posters, and participants as long as the data identifies them. However, the data controller solely specifies and enforces the terms of how the data can be used, and, as a result, has a higher degree of control than the subject. Subjects' control is limited to the right to consent. This right allows the subject to either accept or reject the processing terms of the data controller, as long as the exceptions are not applicable (Article 7(b–f)). This criterion is satisfied to a relatively high degree in terms of controlling different data types of different subject types

as long as exceptions do not apply. However this control is not as granular as the control users have in the technical framework.

Identifiability of the Data Subject: Identifiability in any context is required by the directive to allow subjects to access and receive information about their data when it is to be processed (Articles 10–12). This criterion is satisfied to a high degree.

Audience Control: The directive states that subjects can specify their audience within the social software. Also, subjects have a limited degree of control over the data controller — by the right to consent — who controls external audiences, and processors. Also, the directive does not offer control to audience members over subjects. This criterion is satisfied to a high degree in terms of controlling audience within the social software users, and to a moderate degree in relation to controlling functional entities and external audiences. It is not satisfied in terms of the audience controlling their subjects.

Control of Context: this criterion is satisfied to a high degree in terms of controlling any context by the right to consent.

Degree of Functional Surveillance: the access control regulations involve a high degree of functional surveillance. The data controller is the functional entity responsible for the enforcement of the control offered to subjects. The controller specifies the terms of data processing, and has access to all the data to enforce the terms. Additionally, external functional entities can access the data to conduct certain investigations. In such cases, the monitoring or surveillance of subjects facilitates performing the investigation tasks. Such surveillance is explicitly exempted from being reported to subjects (Article 13(f)). The degree of functional surveillance is higher than the degree of functional surveillance in the technical framework.

4.2.2 *Evaluating Accountability*

The satisfaction of the criteria varies as discussed in the following.

Control over Data: The regulations oblige the data controller to inform data subjects of how their data are used. If the processing does not comply to what the subject has consented to, the subject can complain. If the exception of (Article 13) applies, subjects may not be entitled to this right. And subjects have no right to know why their data is being processed and by whom. This criterion is satisfied to a high degree in terms verifying the observance of control over all data types as long as exemptions do not apply.

Identifiability of the Data Subject: Identifiability is required by the accountability regulations to facilitate identifying subjects who are accountable for misconduct. This criterion is satisfied to a higher degree than the degree of satisfaction in the technical framework.

Audience Control: The directive allows subjects to verify how their data is being processed by the controller or the processor, as long as exceptions are not applicable. Thus, subjects can verify the observance of the control they have over their data by functional entities and external audiences (Article 3(2)). This criterion is satisfied to a high degree in terms of verifying the control over functional entities and external audiences, but it is not satisfied in terms of verifying the control of the audience on subjects.

Control of Context: Through the obligation of informing the subjects about the purpose of processing data (Articles 10–11), subjects can be aware of contexts their data is put in. Subjects, however, cannot limit the processing of data in a specific context if they have given their consent or if the processing is necessary (Article 7). This criterion is satisfied to a moderate degree with regards to verifying subjects' limited control over internal and external contexts.

Degree of Functional Surveillance: to verify the observance of terms of processing by the data controller and the processor, a high degree of functional surveillance is required. Such functional surveillance is performed by external functional entities and legal authorities that access all data available about subjects, the data controller, and the data processors. As a result, the accountability regulations entail a high degree of functional surveillance.

In summary, the legal framework involves a high degree of surveillance to enforce rules and facilitate the control to users on external entities and contexts. Thus, the degree of privacy achieved in this framework is moderate.

The main difference between the technical and legal framework is the scope of the offered control. The technical framework offers control of variant granularity. Users can express detailed or very simple and coarse-grained control, according to the technical mechanism used. In contrast, the legal framework offers static and large-scale control. The regulations that offer control cannot be changed by users, but they apply on a large scale–within and beyond the social software boundaries. Another difference is that in the technical framework violations are detected sooner than violations in the legal framework. In the legal framework, detecting violations requires checking compliance to regulations by external authorities. Such checking may not occur periodically, as is the case in the technical framework.

5. THE INTERDEPENDENCY OF PRIVACY AND SURVEILLANCE

The interdependency of privacy and surveillance is inherent in the design of data control approaches. In the previous sections, we discussed how functional surveillance is part of data control approaches. Giving users a high degree of control over dissemination contexts, for instance, requires increasing functional surveillance to detect disseminations of data in any context. The interdependency of privacy and surveillance is manifested in how functional surveillance serves offering better privacy, and how privacy aims at mitigating surveillance. In the following, we propose recommendations that are essential when the interdependency is present in an approach.

5.1 Recommendations

The variation in the degree of control, privacy and surveillance between PaC approaches in the two frameworks suggest the need for a holistic PaC approach. The variation emerges from the differences in the perspectives and the aspects focused on by an approach. Addressing privacy issues and legal concerns at the same time requires an approach that merges the offerings of the technical and legal frameworks. Developing such an approach requires taking into consideration the interdependency of privacy and surveillance, rather than focusing on only privacy issues [7]. The first step towards developing a better data control approach is adopting transparency and reciprocity.

Transparency is essential to address the dependence of PaC on surveillance. The functional surveillance in data control approaches may turn the social software platforms into a panopticon. In a panopticon setting, individuals should be aware that they are being surveilled. If users are aware of surveillance they can choose what data to disclose in such a platform [16]. Similarly, social software users should be aware of the degree of surveillance in data control approaches [7]. In this case, users can experience being in surveillance spaces and develop appropriate strategies [17] — assuming they are not faced with usability issues of data control approaches.

Reciprocity must be adopted to support transparency. Reciprocity means that if a surveillant entity can monitor users, then users should be able to monitor such an entity [4]. Reciprocity starts with transparency. Once surveillance is transparent, users would able to observe the conduct of the surveilling entity. Reciprocity can be replaced by feedback to users about how their data is handled. Feedback is a "privacy as practice" approach [10]. Thus, with reciprocity, users may achieve privacy as practice as well.

5.2 Transparency and Reciprocity in Practice

As an example of the benefit of transparency and reciprocity, consider the case of Facebook use in Syria. Facebook and Youtube were blocked in Syria until after the uprising in Egypt. The uprising in Egypt coincided with Facebook calls for demonstrations in Syria. At that point, the ban was lifted as a reward for the people who did not respond to the calls [19, 18]. This meant that individuals need not use Tor anonymous communication networks [8]. Without Tor proxies, the identities and communication of individuals will be known to the ISP [12]. Such unintentional transparency and reciprocity about the potential behaviour of the authorities made it clear for activists that the motivation for the lift of the ban could be to prevent anonymous communication and to surveil individuals — given the history of the country. Later reports suggest that surveillance was the reason for the ban was being lift [22]. In this scenario, it is the knowledge about potential surveillance that can empower individuals to carefully use social software and select what to disclose, following the recommendation of McGrath [17]. Such a change of behaviour is also observed in the spike of web searches about surveillance after Snowden's revelations [21]. After the revelations about possible surveillance by the government, searches about surveillance were increased. The increase indicates that users were interested in gaining more knowledge about how surveillance can be applied, avoided, etc.

6. RELATED WORK

Similar analyses of privacy management approaches have been conducted earlier. In the technical framework, Danezis and Gürses provide a review of privacy technologies and highlight the entanglement of privacy and surveillance in technologies [7]. Their review covers a wide selection of technologies developed between 2000 and 2010, but mainly focuses on anonymous communication and identity management technologies. Their review argues that total control of data is an illusion, and that privacy technologies can be turned into surveillance tools. While their review focuses on the three privacy paradigms — privacy as control, privacy as confidentiality and privacy as practice — our work differs in focusing just on privacy as control (PaC). Our work extends the analysis of PaC to the legal framework. Our work also differs in conceptualising functional surveillance as one factor that facilitates using technologies for surveillance. Another difference is our proposed criteria that can be applied on any approach to assess the degree of control and surveillance. The criteria can be applied on anonymous communication, identity management approaches, or any other approach within PaC.

In another work, Gürses and Diaz focus on surveillance and social privacy issues in social software [12]. These issues relate to the aspects discussed in our work. Data control approaches facilitate social privacy management to avoid violations and surveillance. The authors argue that surveillance and social privacy issues are entangled, and that privacy management approaches should not address one of these issues and ignore the other. We also examine data control approaches comprehensively and show that this entanglement is a functional requirement for data control approaches. We argue that aiming to give as much control as possible to users may not address this entanglement, since functional surveillance is a fundamental aspect of data control approaches. Our work also differs in that we consider data control approaches in the legal framework, while Gürses and Diaz do not focus on data protection regulations. The questions proposed by Gürses and Diaz for eliciting information useful to developing a holistic privacy management approach can be integrated with our proposed criteria. Such an integration provides detailed information towards developing holistic approaches.

The concept of functional surveillance has been examined by other authors. The work of Gurevich *et al.* conceptualises *'inverse privacy'* [9] that relates to our conceptualisation of functional surveillance. Inverse privacy refers to the concept of collecting information about users without their knowledge. *Inversely private data* is data that the user is unaware of, yet, it is accessed by entities unknown to the user in a way that can be inappropriate. In our work, functional surveillance facilitates inverse privacy by facilitating the collection of information about users' actions and usage of data control approaches. Our proposed criteria can be applied to assess the degree of inverse privacy.

7. CONCLUSION AND FUTURE WORK

In PaC, users cannot control their data without relying on the control of functional entities. In the comparative analysis presented in this article, we show the complementarity between access control and accountability. We also show the variation in the realisations of PaC in the technical and the legal frameworks. The realisations of data control approaches offer varying degrees of control and functional surveillance. These offerings result in an interdependency of privacy and surveillance. The analysis explicates the reasons for this interdependency.

The application of the proposed criteria is promising for the assessment of the degree of privacy and the degree of surveillance of a specific approach. Such an assessment is fundamental and should not be skipped by researchers. Using the criteria would decrease developing approaches that address certain privacy issues and cause others, such as surveillance. The criteria should be adopted to decrease the ambiguity about the degree of control and privacy an approach can offer. As well as making clear the possible

surveillance aspect that may result from adopting a particular data control approach.

In the future work, we aim at providing an example for developing a data control approach and assessing the possible degree of control, privacy and surveillance it offers. We aim at developing our previously-proposed contextual privacy management framework and using the proposed criteria to assess it [25]. The framework is designed to comply with the data control aspects discussed in this paper to offer fine-grained control over context. We plan to provide an example of how the criteria can be applied on a particular approach. We also seek to investigate possible quantification methods of the degree of control, privacy and surveillance. The main objective of this work, and future work, is to provide a method to investigate privacy and the other side of privacy, surveillance in data control approaches.

Acknowledgment

This research has been funded by the IWT in the context of the SBO project on Security and Privacy for Online Social Networks (SPION). Thanks are due to Sören Preibusch at Microsoft Research Cambridge.

8. REFERENCES

[1] A. Acquisti, E. Balsa, B. Berendt, D. Clarke, W. De Groef, R. De Wolf, C. Diaz, B. Gao, S. Gürses, J. Pierson, F. Piessens, R. Sayaf, T. Schellens, F. Stutzman, B. Van Alsenoy, and E. Vanderhoven. SPION project deliverable. D2.1-state of the art, 2010.

[2] J. Alhadeff, B. Van Alsenoy, and J. Dumortier. The accountability principle in data protection regulation: Origin, development and future directions. In D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland, and H. Postigo, editors, *Managing privacy through accountability*. Palgrave Macmillan, Basingstoke, UK, 2012.

[3] S. B. Barnes. A privacy paradox: Social networking in the united states. *First Monday*, 11(9), 2006.

[4] A. Clement. Considering privacy in the development of multi-media communications. *Computer Supported Cooperative Work*, 2(1-2):67–88, 1993.

[5] E. Commission. Article 29 data protection working party, opinion 5/2009 on online social networking. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf, 2009.

[6] L. Cutillo, R. Molva, and T. Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. *Communications Magazine, IEEE*, 47(12):94 –101, dec. 2009.

[7] G. Danezis and S. Gürses. A critical review of 10 years of privacy technology. In *Surveillance Clutures: A Global Surveillance Society*, 2010.

[8] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In *USENIX Security Symposium*, pages 303—320, 2004.

[9] Y. Gurevich, H. E., and J. Wing. Inverse privacy. Technical report, Microsoft Research, 2014.

[10] S. Gürses. *Multilateral Privacy Requirements Analysis in Online Social Network Services*. PhD thesis, KU Leuven, 2010.

[11] S. Gürses and B. Berendt. PETS in the surveillance society: A critical review of the potentials and limitations of the privacy as confidentiality paradigm. In *Data Protection in a Profiled World*, pages 301–321. Springer, 2010.

[12] S. Gürses and C. Diaz. Two tales of privacy in online social networks. *IEEE Security & Privacy*, 11(3):29–37, 2013.

[13] A. Haeberlen and P. Kouznetsov. Peerreview: practical accountability for distributed systems. In *Proceedings of twenty-first ACM SIGOPS symposium on Operating systems principles*, SOSP '07, pages 175–188, NY, USA, 2007. ACM.

[14] R. Harper, editor. *Trust, Computing and Society*. CUP: New York, 2014.

[15] G. Karjoth, M. Schunter, and M. Waidner. Platform for enterprise privacy practices: Privacy-enabled management of customer data. In *Privacy Enhancing Technologies*, pages 69–84. Springer, 2003.

[16] J. E. Katz and R. E. Rice. *Social consequences of Internet use: Access, involvement, and interaction*. MIT press Cambridge, MA, 2002.

[17] J. McGrath. *Loving Big Brother: Performance, privacy and surveillance space*. Psychology Press, 2004.

[18] B. Mroue. Syria Facebook, YouTube Ban Lifted: Reports. The World Post, Feb. 2011.

[19] I. on Censorship. Syria unblocks Facebook and Youtube. Electronic article: http://www.indexoncensorship.org/2011/02/syria-unblocks-facebook-and-youtube/, Feb. 2011.

[20] D. M. Pedersen. Model for types of privacy by privacy functions. *Journal of Environmental Psychology*, 19(4):397 – 405, 1999.

[21] S. Preibusch. Privacy behaviors after snowden. *Commun. ACM*, 58(5):48–55, Apr. 2015.

[22] J. Preston. Seeking to disrupt protesters, Syria cracks down on social media. Electronic article: http://www.nytimes.com/2011/05/23/world/middleeast/23facebook.html, May 2011.

[23] J. B. Rule. When it comes to protecting its citizens' data, Europe is way ahead of the U.S. http://www.latimes.com/opinion/op-ed/la-oe-rule-nsa-privacy-european-union-20140513-story.html, May 2014.

[24] R. Sayaf and D. Clarke. Access control models for online social networks. *Social Network Engineering for Secure Web Data and Services*, pages 32–65, 2012.

[25] R. Sayaf, D. Clarke, and R. Harper. CPS^2: a contextual privacy framework for social software. In *SECURECOMM 2014*. Springer, 2014.

[26] R. Sayaf, J. B. Rule, and D. Clarke. Can users control their data in social software? an ethical analysis of data control approaches. In *IEEE S& P Workshops (SPW)*, pages 1–4, 2013.

[27] B. Schneier and J. Kelsey. Secure audit logs to support computer forensics. *ACM Trans. Inf. Syst. Secur.*, 2:159–176, May 1999.

[28] A. Simpson. On the need for user-defined fine-grained access control policies for social networking applications. *Proceedings of the workshop on Security in Opportunistic and SOCial networks - SOSOC '08*,

pages 1–8, 2008.

[29] A. C. Squicciarini, M. Shehab, and J. Wede. Privacy policies for shared content in social network sites. *The VLDB Journal—The International Journal on Very Large Data Bases*, 19(6):777–796, 2010.

[30] A. C. Squicciarini and S. Sundareswaran. Web-traveler policies for images on social networks. *World Wide Web Internet And Web Information Systems*, 12(4):461–484, 2009.

[31] C. Wang and H.-f. Leung. A secure and private clarke tax voting protocol without trusted authorities. In *Proceedings of the 6th international conference on Electronic commerce*, ICEC '04, pages 556–565, New York, NY, USA, 2004. ACM.

[32] S. Warren and L. Brandeis. The right to privacy. *Harward Law Review*, 4(5):193—220, 1890.